IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, et al.,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT, et al.,

Defendants.

Case No. 25-cv-1237-DLC

DECLARATION OF GREGORY J. HOGAN

I, Gregory J. Hogan, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury as follows:

1. I am currently employed by the United States Office of Personnel Management ("OPM"), as the Chief Information Officer ("CIO") of OPM. I was onboarded at OPM as a Senior Advisor to the Director (of OPM) for Technology and Delivery on January 20, 2025, and I served as the Acting CIO from that date through February 12, 2025, when I was appointed to the permanent CIO position. Before joining OPM, I served as Vice President of Infrastructure at comma.ai. I have more than 20 years of experience in the private sector in information technology and a degree in Computer Engineering.

2. In my role at OPM, I have the following responsibilities pursuant to 40 U.S.C. § 11315:

a. I am responsible for the development and maintenance of OPM's IT and information resources infrastructure.

b. I advise agency leadership regarding the acquisition and management of IT resources.

c. I advise agency leadership regarding the acquisition and management of IT resources.

3. I make this declaration based on my personal knowledge and on information contained in OPM's files, or information provided to me in the course of performing my duties, including information provided by OPM's Chief Information Security Officer (CISO) and OPM's human resources (HR) department.

4. The purpose of this declaration is to (i) supplement my previous declaration submitted in this matter, dated February 19, 2025, (ii) provide information about access to and safeguarding of OPM's data systems, and (iii) respond to erroneous information contained in the complaint, briefing, and declarations filed by Plaintiffs in this action.

5. Most of OPM's data systems are run on, or are accessed through, Microsoft's Azure platform, which utilizes the Microsoft Entra ID identity and access management solution to manage accounts and access to these data systems.[1] With respect to such systems, normal user identity and user access management is achieved through certificate-based authentication, where an OPM user is required to insert a government-issued personal identity verification (PIV) card into a card reader on a government furnished laptop (also known as government furnished equipment or GFE), enter a personal identification number (PIN), and authenticate using the security certificate stored on the PIV card. For new OPM employees or those OPM employees with temporary appointments, the Office of the Chief Information Officer ("OCIO") issues

[1] An overview of Microsoft Entra ID may be found here: *See* Cybersecurity & Infrastructure Security Agency, *Microsoft Entra* ID, https://www.cisa.gov/resources-tools/services/m365-entra-id. Microsoft Azure Government is authorized by the Federal Risk and Authorization Management Program (FedRAMP) at the High impact level, referring to authorization of cloud services for federal government use in connection with the most sensitive, unclassified data, and has been granted Authority to Operate (ATO) across dozens of federal agencies. *See* FedRAMP, https://marketplace.fedramp.gov/products/F1603087869.

temporary local area network ("LAN") credentials, that are used for logical access to OPM's data systems.[2] OCIO issued temporary LAN credentials and GFE laptops to new OPM appointees (including myself) during onboarding.

6. Utilizing a temporary LAN credential or PIV card is an example of multi-factor authentication, because it requires a physical card, a separate PIN, as well as utilization of GFE to access these systems.

7. OPM uses the Microsoft Entra ID identity and access management solution to manage user and administrator privileged roles and permissions with respect to most of OPM's data systems—including systems such as USAJOBS and data systems such as EHRI. *See, e.g.*, OPM-000104; OPM-000092.[3] *See* Cybersecurity & Infrastructure Security Agency, *Microsoft Entra* ID, https://www.cisa.gov/resources-tools/services/m365-entra-id. OPM utilizes Entra ID's role-based access control to assign roles to grant access, use groups to manage role assignments, create administrative units to restrict scope, or create custom roles with specific permissions. OPM also utilizes Entra ID to assign individual employees with varying privileged roles and permissions on OPM's systems, based on the individual's need for access.[4]

8. Utilization of PIV credentials or temporary credentials in conjunction with Microsoft Entra ID is the principal way in which OPM ensures appropriate account management

[2] Temporary LAN credentials are physical cards that function similarly to a PIV card, require a PIN, and are used with the card reader on GFE laptops, except the security certificate stored on the temporary LAN credential is only valid for up to 6 months, and the temporary credential does not have a photograph, name, or other identifying details—so the physical card may be recycled and repurposed for future employees.

[3] Microsoft Entra ID was formerly known as Azure Active Directory (Azure AD), and the latter name is still used in the Azure platform. *See* https://learn.microsoft.com/en-us/entra/fundamentals/new-name; OPM-000092 ("Azure AD Identity Governance - Directory Management").

[4] Entra ID allows for many different types of "administrator access" based on different roles and associated permissions. *See, e.g.*, https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-roles-permissions; https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles. Entra ID does not utilize terms such as "root access," or "God Mode."

and access enforcement, enforcing approved authorizations for logical access to information and system resources in accordance with applicable policies. *See* National Institute of Standard and Technology (NIST), *Security and privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (SP800-53, Rev. 5), AC-2 and AC-3.[5] Utilization of Entra ID is also one way in which OPM implements the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. *See* NIST SP800-53, Rev. 5, AC-6. OPM accomplishes this by assigning specific users to specific groups or roles in Entra ID that correspond to pre-set permissions.

9. In connection with OPM's use of Entra ID access control, an individual user granted "administrator access" or "administrative access" means that that individual was assigned to a role with permissions allowing them to perform certain functions that a regular user would not be able to perform—and the types of functions authorized vary depending on the particular role at issue. *See* NIST SP800-53, Rev. 5, AC-2(7) ("Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform."). The granting of permissions to access a specific system—i.e., creating an account for that system—does not mean that the particular individual granted that permission actually logged in and accessed any data in that system. It also does not mean that individual has the highest and most powerful level of access to a data system. And it does not mean that a user with such access can necessarily (1) permanently delete critical data owned by and affecting other users, (2) disable, modify, or destroy data

[5] NIST, a component of the U.S. Department of Commerce, is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST SP800-53, Rev. 5 is publicly available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

backups, (3) disable logging or audit trails used to conduct forensic analysis, or (4) take OPM's data systems fully offline. I am not aware of anyone at OPM taking the above actions, or even requesting that they be taken, while I have been employed at OPM.

10. Another important aspect of the principle of least privilege is the periodic review of assigned user privileges to determine if the rationale for assigning such privileges remains valid. *See* NIST SP800-53, Rev. 5, AC-6(7). OPM implements this aspect of the principle of least privilege by periodically reviewing of assigned user privileges and taking corrective action by removing privileges where necessary to correctly reflect OPM's mission needs. For example, on February 6, 2025, I requested information on whether certain individuals were granted access to certain systems and to remove access if it was currently unnecessary. *See* OPM-000027. I instructed OPM's associate CIO to remove access to EHRI and eOPF for those individuals. *See* OPM-000026. I was informed that while accounts had been created for certain of those individuals for EHRI and eOPF—i.e., they had been assigned permission for those systems in Entra ID—those individuals had never utilized those accounts, no longer needed access, and those permissions were subsequently disabled. *See* OPM-000023-26. On February 16, 2025, I requested additional information and received an account creation audit, showing all accounts created at OPM from January 20, 2025, through February 12, 2025. *See* OPM-000089-91.

11. OPM's CISO team undertook a review of account access for myself, Charles Ezell, Amanda Scales, and individuals identified as OPM-2 through OPM-18, for the period including January 20, 2025 through March 6, 2025, which is included in the administrative record at OPM-000103. This review showed that none of these users had actually logged into EHRI or eOPF during this time period. *See* OPM-000103 (showing that no users actually accessed EHRI and eOPF).

12. I understand that Plaintiffs have claimed that "DOGE agents used the EHRI and eOPF databases to create a government-wide email system," and they cite to the Privacy Impact Assessment for the GWES included at OPM-000119 ("The GWES is built largely upon employee email contact information found in the Enterprise Human Resources Integration (EHRI) and Official Personnel Folder (OPF) record systems."). While the government email addresses and names used to send emails through the GWES do come from EHRI and eOPF, those data elements were supplied by career OPM staff who extracted those data elements from the EHRI data warehouse. That information was requested to send emails through the GWES, which uses the names and email addresses of federal government employees. *See* OPM-000121. These data elements do not contain personal information about an individual beyond their name and agency. Furthermore, despite erroneous news reporting to the contrary, no one has connected a "private server" to any OPM system to control the GWES or any other personnel databases—including any on-premises data systems.[6] As detailed above, most of OPM's data systems are accessed only through the FedRAMP approved Microsoft Entra ID, and all cloud-based systems are run on the FedRAMP approved Microsoft Azure platform.

13. Seventeen individuals were also granted permissions to access USA Performance, but prior to March 6, 2025, these individuals had not actually logged into that system and did not access any underlying personal data contained in the system. *See* OPM-000103. Moreover, none of these individuals (except for myself) actually logged into the USA Performance system as of March 6, 2025, and user access is automatically revoked after 60 days of inactivity.

[6] As outlined in the GSES Privacy Impact Assessment, "The GWES is located within Microsoft applications and on secure government computers. These Microsoft Applications have been granted an Authorization to Operate (ATO) that includes an approved system security plan. The government computers storing the data are subject to standard security requirements, including limited PIV access." OPM-000120. This refers to operation of the GWES on the Microsoft Azure platform that has a FedRAMP High impact level ATO.

14. The only OPM data system which any of the relevant individuals actually logged into prior to March 6, 2025, was the USA Staffing platform. *See* OPM-000103 (showing four individuals who logged into USA Staffing). Of those individuals, Amanda Scales was the prior Chief of Staff to the Director of OPM, James Sullivan is the current Chief of Staff to the Director of OPM, OPM-7 is a Senior Advisor to the Director of OPM, and OPM-6 was an expert computer engineer who assisted with software development work on the USA Staffing platform. These OPM employees were provided with this type of "administrative access" for several reasons, including so that they could make system changes in connection with automated hiring/onboarding and job posting processes, in furtherance of their duties in carrying out the President's executive order implementing a government-wide hiring freeze, *see* Presidential Memorandum, *Hiring Freeze* (Jan. 20, 2025), 90 Fed. Reg. 8247-48, and so that they could develop and implement a data-driven Federal Hiring Plan pursuant to executive order, *see* Executive Order 14,170 (Jan. 20, 2025), 90 Fed. Reg. 8,621.

15. OPM has consistently followed appropriate safeguards in connection with the granting of access permissions to OPM data systems to individuals who onboarded on or after January 20, 2025.

Dated: May 16, 2025
Washington, D.C.
.

Gregory J Hogan
Gregory J. Hogan